The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
5/11/2012

SUBJECT:
Multiple Vulnerabilities in Apple Mac OS X

OVERVIEW:
Multiple vulnerabilities have been discovered in Apple‘s Mac OS X and Mac OS X Server that could allow remote code execution. Mac OS X is a desktop operating system for the Apple Mac. Mac OS X Server is a server operating system for the Apple Mac.

These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file, including an email attachment, using a vulnerable version of OS X. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
Apple OS X Lion 10.7.3 and earlier
Apple OS X Server v10.7.3 and earlier

RISK:
Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
Multiple vulnerabilities have been discovered in Apple Mac OS X that could allow remote and local code execution, denial-of-service conditions, unauthorized access, information disclosure, and the bypass of security restrictions. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file, including an email attachment, with a vulnerable version of Apple Mac OS X.

Apple has identified the following vulnerabilities:

A vulnerability exists in the Login Window of Mac OS X Lion and Lion Server v10.7.3. The vulnerability is caused by the way OS X handles network account logins. When logging into the system, sensitive information is recorded in the system log, which can later be accessed by other users. Please note that the sensitive information will still exist in the saved logs on the system even after the update is applied. (CVE-2012-0652)

A local privilege escalation vulnerability exists in Mac OS X Lion and Lion Server v10.7 – v10.7.3. The issue exists in their Bluetooth application Blued. A race condition exists in Blued's initialization routine that could allow a user to execute arbitrary code with system privileges. (CVE-2012-0649)

A vulnerability exists in the curl application which could allow for information disclosure due to the way curl is configured. Curl disabled the "empty fragment" countermeasure that would allow an attacker to decrypt data protected by SSL. This issue affects Mac OS X 10.6.8, Mac OS X Server 10.6.8, OS X Lion v10.7 to v10.7.3, OS X Lion Server v10.7 to v10.7.3. (CVE-2011-3389)

A second vulnerability exists in the curl application that could lead to protocol-specific data injection attacks. The issue is triggered because of the way curl handles URLs. Note, that this issue does not affect systems prior to OS X Lion. This issue affects OS X Lion v10.7 to v10.7.3, OS X Lion Server v10.7 to v10.7.3. (CVE-2012-0036)

A vulnerability exists in Directory Service which can be exploited to obtain sensitive information. To leverage this issue, an attacker would send a specially crafted message to the directory server that will disclose memory from its address space. This issue does not affect OS X Lion systems. The Directory Server is disabled by default in non-server installations of OS X. This issue affects Mac OS X 10.6.8, Mac OS X Server 10.6.8. (CVE-2012-0651)

A remote code execution vulnerability exists in the Hierarchical File System (HFS) due to an integer underflow in the handling of HFS catalog files. HFS is a file system developed by Apple for use in systems running Mac OS. To exploit this issue and attacker would have to trick a user into mounting a maliciously crafted disk image. This issue affects OS X Lion v10.7 tov10.7.3, OS X Lion Server v10.7 to v10.7.3.

Two vulnerabilities exist in ImageIO that could lead to remote code execution. ImageIO provides interfaces for importing and exporting image data and image metadata. Both issues are caused by viewing a maliciously crafted TIFF file that triggers a buffer overflow in ImageIO. Successful exploitation could lead to remote code execution or denial of service conditions. These issues affect Mac OS X v10.6.8, Mac OS X Server v10.6.8. (CVE-2011-0241, CVE-2011-1167)

Two denial of service vulnerabilities exist in libpng. The first issue is due to a divide-by-zero bug in png_handle_cHRM(), which could lead to denial of service in applications that support color correction. The second issue is called libpng read uninitialized memory when handling empty sCAL chunks, and they handle malformed sCAL chunk incorrectly. These issues affect Mac OS X 10.6.8, Mac OS X Server 10.6.8. (CVE-2011-2692, CVE-2011-3328)

An information disclosure vulnerability exists in the Mac OS X kernel's handling of the sleep image used for hibernation. When hibernation is used it causes some data to be left unencrypted on the disk even when file vault is enabled. This issue affects OS X Lion v10.7 to v10.7.3, OS X Lion Server v10.7 to v10.7.3. (CVE-2011-3212)

Two remote code execution vulnerabilities exist in libarchive due to the way it handles tar archives and iso9660 files. An attacker could exploit this issue by tricking a user into extracting a maliciously crafted archive that would cause a buffer overflow condition and lead to remote code execution or denial of service conditions. This issue affects Mac OS X 10.6.8, Mac OS X Server 10.6.8, OS X Lion v10.7 to v10.7.3, OS X Lion Server v10.7 to v10.7.3. (CVE-2011-1777, CVE-2011-1778)

A remote code execution vulnerability exists in libsecurity due to the way it handles X.509 certificates. The issue is triggered when libsecurity attempts to verify a specially crafted X.509 certificate when visiting a malicious website. This issue affects Mac OS X 10.6.8, Mac OS X Server 10.6.8, OS X Lion v10.7 to v10.7.3, OS X Lion Server v10.7 to v10.7.3. (CVE-2012-0654)

An information disclosure vulnerability exists in libsecurity because it accepts insecure RSA keys. This issue affects Mac OS X 10.6.8, Mac OS X Server 10.6.8, OS X Lion v10.7 to v10.7.3, OS X Lion Server v10.7 to v10.7.3. (CVE-2012-0655)

Multiple remote code execution vulnerabilities exist in libxml. These issues can be triggered by viewing a malicious website. These issues affect Mac OS X 10.6.8, Mac OS X Server 10.6.8, OS X Lion v10.7 to v10.7.3, OS X Lion Server v10.7 to v10.7.3. (CVE-2011-1944, CVE-2011-2821, CVE-2011-2834, CVE-2011-3919)

A security bypass vulnerability exists in the LoginUIFramework which could allow unauthenticated local access to a machine. If the Guest user account is enabled, an unauthenticated attacker may be able to login as another user without supplying credentials. This issue affects OS X Lion v10.7 to v10.7.3, OS X Lion Server v10.7 to v10.7.3). (CVE-2012-0656)

Multiple vulnerabilities exist in PHP that could cause remote code execution or denial of service conditions. These issues affect OS X Lion v10.7 to v10.7.3, OS X Lion Server v10.7 to v10.7.3. (CVE-2011-4566, CVE-2011-4885, CVE-2012-0830)

A security bypass vulnerability exists in Quartz Composer which could allow an unauthenticated user to launch Safari if the screen is locked and the RSS Visualizer screen saver is used. Quartz composer is a node-based visual programming language provided as part of the Xcode development environment in Mac OS X. The issue is caused by the way Quartz Composer handles screen savers while the system is locked. This issue affects Mac OS X 10.6.8, Mac OS X Server 10.6.8, OS X Lion v10.7 to v10.7.3, OS X Lion Server v10.7 to v10.7.3. (CVE-2012-0657)

Multiple remote code execution vulnerabilities exist in QuickTime. These issues can be exploited if a user opens a specially crafted movie or MPEG file designed to leverage these issues. Mac OS X 10.6.8, Mac OS X Server 10.6.8, OS X Lion v10.7 to v10.7.3, OS X Lion Server v10.7 to v10.7.3 are affected. (CVE-2012-0658, CVE-2012-0659, CVE-2012-0660, CVE-2012-0661)

Multiple vulnerabilities exist in Ruby that cause denial of service, information disclosure, and modify information. This issue affects Mac OS X 10.6.8, Mac OS X Server 10.6.8, OS X Lion v10.7 to v10.7.3, OS X Lion Server v10.7 to v10.7.3. (CVE-2011-1004, CVE-2011-1005, CVE-2011-4815)

Multiple vulnerabilities exist in Samba that can cause remote code execution and denial of service conditions. These issues are due to the way Samba handles remote procedure calls. An attacker could leverage this by sending a maliciously crafted packet to a vulnerable machine. These issues affect Mac OS X 10.6.8, Mac OS X Server 10.6.8. (CVE-2012-0870, CVE-2012-1182)

An integer overflow vulnerability in the Security Framework could cause remote code execution. This vulnerability is caused by the way the Security Framework processes un-trusted input. Note that this vulnerability does not affect 32 bit processes. This issue affects Mac OS X 10.6.8, Mac OS X Server 10.6.8, OS X Lion v10.7 to v10.7.3, OS X Lion Server v10.7 to v10.7.3. (CVE-2012-0662)

An information disclosure vulnerability has been discovered in Time Machine. Time Machine is Apple’s backup utility. This vulnerability can be leveraged by an attacker who is able to spoof the remote volume. They may be able to access a user's Time Capsule credentials that are sent by the user's system. This vulnerability is caused because Time Machine only requires the SRP-based authentication credentials to be supplied for the first backup. This issue affects OS X Lion v10.7 to v10.7.3, OS X Lion Server v10.7 to v10.7.3. (CVE-2012-0675)

A buffer overflow vulnerability exists in X11 which can cause remote code execution and denial of service conditions. Any applications that use libXfont to process LZW-compressed data may be vulnerable. This issue affects OS X Lionv10.7 to v10.7.3, OS X Lion Server v10.7 to v10.7.3. (CVE-2011-2895)

Successful exploitation of any of these remote code execution vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed attempts could result in a denial-of-service.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Apple to affected systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Permit local access for trusted individuals only. Where possible, use restricted environments and restricted shells.
- Remind users not to download or open files from un-trusted websites.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Remind users not to click links from unknown sources, or to click links without verifying the intended destination.

REFERENCES:
Apple:
http://support.apple.com/kb/HT5281

Security Focus:
http://www.securityfocus.com/bid/53445
http://www.securityfocus.com/bid/53457
http://www.securityfocus.com/bid/53456
http://www.securityfocus.com/bid/53458
http://www.securityfocus.com/bid/53471
http://www.securityfocus.com/bid/53462
http://www.securityfocus.com/bid/53459
http://www.securityfocus.com/bid/53473
http://www.securityfocus.com/bid/53465
http://www.securityfocus.com/bid/53467
http://www.securityfocus.com/bid/53469
http://www.securityfocus.com/bid/53466
http://www.securityfocus.com/bid/53468
http://www.securityfocus.com/bid/53470

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0652
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0649
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3389

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0036
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0651
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0642
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0241
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2692
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3328
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1167
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3328
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1167
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3212
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1777
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1778
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0654
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0655
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1944
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2821
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2834
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3919
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0656
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4556
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4885
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0830
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0657
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0658
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0659
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0660
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0661
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1004
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1005
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4815
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0870
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1182
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0662
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0675
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2895